REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2009	FINAL	

4. TITLE AND SUBTITLE

Integrating Intelligence and Information Sharing in Theater Security Cooperation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Robert T. Flickinger, USN

Paper Advisor (if Any): CDR Mark Houff, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Theater Security Cooperation plans and activities are essential in developing capable coalition partners that work with the United States to maintain regional stability and counter common threats. A critical component of Theater Security Cooperation planning is intelligence and information sharing. This paper explores how Operational Function Intelligence should be integrated into Theater Security Cooperation and campaign planning in order to most effectively support the Geographic Combatant Commander. It begins with an examination of the strategic level guidance that lists a Geographic Combatant Commander's intelligence and information sharing responsibilities. It explains the value of intelligence and information sharing with foreign partners and how intelligence and information sharing supports multinational operations. It recognizes intelligence and information sharing challenges and identifies potential ways to mitigate these challenges. Finally, the paper draws conclusions concerning the nature of intelligence and information sharing relationships and recommends ways that a Geographic Combatant Commander's Director for Intelligence could improve the efficiency and effectiveness of intelligence sharing activities.

15. SUBJECT TERMS

Intelligence Sharing, Information Sharing, Security Cooperation, Foreign Partners

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		28	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Integrating Intelligence and Information Sharing in Theater Security Cooperation

by

Robert T. Flickinger

Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

04 May 2009

Contents

Introduction	1
Theater Security Cooperation Planning Guidance	2
Value of Sharing Intelligence and Information	6
Intelligence Sharing Challenges	8
The Case against Sharing Intelligence	13
Conclusions	14
Recommendations	15
Notes	18
Bibliography	21

Abstract

Integrating Intelligence and Information Sharing in Theater Security Cooperation

Theater Security Cooperation plans and activities are essential in developing capable coalition partners that work with the United States to maintain regional stability and counter common threats. A critical component of Theater Security Cooperation planning is intelligence and information sharing. This paper explores how Operational Function Intelligence should be integrated into Theater Security Cooperation and campaign planning in order to most effectively support the Geographic Combatant Commander. It begins with an examination of the strategic level guidance that lists a Geographic Combatant Commander's intelligence and information sharing responsibilities. It explains the value of intelligence and information sharing with foreign partners and how intelligence and information sharing supports multinational operations. It recognizes intelligence and information sharing challenges and identifies potential ways to mitigate these challenges. Finally, the paper draws conclusions concerning the nature of intelligence and information sharing relationships and recommends ways that a Geographic Combatant Commander's Director for Intelligence could improve the efficiency and effectiveness of intelligence sharing activities.

INTRODUCTION

Intelligence and information sharing with allies and foreign partners is a critical component of Theater Security Cooperation (TSC) that must be given greater focus by Geographic Combatant Commanders (GCCs) and their Directors for Intelligence (J-2s).[1] Lack of emphasis on intelligence sharing during security cooperation and campaign planning has resulted in the inability to fully leverage exchange programs with many foreign partners.

GCCs conduct security cooperation planning in support of campaign plans as directed by the Guidance for Employment of the Force (GEF) and the Joint Strategic Capabilities Plan (JSCP).[2] The J-2 must coordinate with the Director for Plans (J-5) to ensure intelligence sharing is made a priority in the overall security cooperation and campaign planning process. J-2s should also work to incorporate intelligence sharing into bilateral and combined exercises making sure it is practiced at every opportunity.

GCCs have intelligence sharing agreements with the armed forces of many countries. The agreements, while coordinated with several U.S. Intelligence Community agencies, are separate from national-level intelligence sharing agreements maintained by those agencies. The J-2 manages the GCC's intelligence sharing agreements and works to build professional and personal relationships with foreign counterparts. Intelligence sharing agreements are important because they give GCCs the opportunity to use foreign partner intelligence assets, capabilities, and analysis in support of multinational operations. Intelligence sharing agreements also provide access to unique sources of information, specifically Human Intelligence (HUMINT) which is extremely valuable in combating terrorism, conducting counter-insurgency, and other missions across the Range of Military Operations (ROMO).

Intelligence sharing is not an easy task and several challenges must be addressed. Intelligence sharing relationships must be built on trust and take a significant amount of time to develop. Cultural differences can cause misunderstandings and language differences can limit communications. Complex foreign disclosure policies and processes cause inefficiencies and limit intelligence dissemination. Secure and interoperable information systems are not always available to foreign partners. Some foreign partner militaries have a service-centric organizational structure with no direct J-2 counterpart. Furthermore, some foreign partners lack training on U.S. security procedures and do not understand the importance of protecting intelligence reporting, sources, and methods. Finally, counterintelligence threats exist, especially when trust has not been developed over time. In order to overcome these challenges, J-2s will have to invest time and dedicate additional personnel and resources. The U.S. Defense Attaché can also help J-2s build intelligence sharing relationships and assist in mitigating some of the challenges.

THEATER SECURITY COOPERATION PLANNING GUIDANCE

The requirements to conduct security cooperation and campaign planning are articulated in numerous national level and Department of Defense (DoD) documents. The National Security Strategy (NSS), National Defense Strategy (NDS), National Military Strategy (NMS), Unified Command Plan (UCP), Guidance for Employment of the Force (GEF), and Joint Strategic Capabilities Plan (JSCP) form the foundation for a GCC's TSC planning and intelligence sharing activities. Other important documents that tangentially impact a GCC's TSC planning and intelligence sharing activities are the Quadrennial Defense Review (QDR), the U.S. Intelligence Community Information Sharing Strategy, the

National Strategy for Information Sharing, and the recently superseded Security Cooperation Guidance (SCG) planning document.[3]

The NSS does not specifically address TSC, but lists "Strengthen Alliances to Defeat Global Terrorism…" and "Develop Agendas for Cooperative Action with the Other Main Centers of Global Power" as essential national tasks.[4] Regarding cooperative action, the NSS recognizes that "there is little of lasting consequence that we can accomplish in the world without the sustained cooperation of our allies and partners."[5] The NDS acknowledges that allies possess capabilities, skills, and knowledge that the U.S. cannot duplicate and explicitly references security cooperation and information sharing by stating, "We will assist other countries in improving their capabilities through security cooperation, just as we will learn valuable skills and information from others better situated to understand some of the complex challenges we face together."[6] The NMS discusses the benefits of security cooperation and intelligence sharing. Regarding intelligence sharing, the NMS states that "achieving shared situational awareness with allies and partners will require compatible information systems and security processes that protect sensitive information without degrading the ability of multinational partners to operate effectively with U.S. elements. Such information and intelligence sharing helps build trust and confidence essential to strong international partnerships."[7] The UCP establishes the missions and responsibilities of combatant commanders. The UCP specifies that GCCs are responsible for "planning, conducting, and assessing security cooperation activities" within their assigned geographic Areas of Responsibility.[8]

The GEF translates concepts in the NSS and NDS into guidance which supports planning and action.[9] The GEF explicitly lists "Intelligence Sharing" with partner nations in

the planning guidance for most areas in the functional, and all areas in the regional chapters. For example, the Intelligence Sharing planning guidance for the *functional* area of Global War on Terrorism states, "Focus on enabling a common understanding of the threat and an improved understanding of the human terrain of relevant populations."[10] The Intelligence Sharing planning guidance for the *regional* area of USAFRICOM states:

> Focus on enabling a common understanding of the threat and an improved understanding of the human terrain of relevant populations. Specifically, focus on countering terrorism, threats to political stability, and proliferation of WMD [weapons of mass destruction] and associated materials. Support information sharing on humanitarian and disaster response issues.[11]

The Intelligence Sharing planning guidance in the regional chapters is tailored to the unique challenges faced by each GCC. A comparison of the above Intelligence Sharing guidance for USAFRICOM with the following guidance for USSOUTHCOM illustrates this point.

> Focus on counter-narcotics, counterterrorism, and political reporting, as well as improving our understanding of the human terrain. Prevent compromise of intelligence and information sharing initiatives and seek to develop a common regional understanding of threats.[12]

Both stress counterterrorism, but USAFRICOM focuses on political stability and understanding local populations while USSOUTHCOM focuses on counter-narcotics.

In 2008, the GEF superseded the SCG as the authoritative document which provides guidance for security cooperation planning. A review of the SCG, however, revealed two key points that are not adequately addressed in the GEF. First, the SCG acknowledges that "security cooperation activities involve an investment that is constrained by forces, funds, and time."[13] This issue will be further examined in the "Intelligence Sharing Challenges" section of this paper. Second, the SCG used the term "Information Sharing/Intelligence Cooperation," which it defined as "activities that increase partner nation intelligence capacity, information sharing and awareness."[14] This term is noteworthy because it implies

cooperation in conducting intelligence analysis, and not just in sharing intelligence reporting, a distinction the GEF fails to make.

The JSCP is the Chairman of the Joint Chiefs of Staff instruction tasking the Geographic and Functional Combatant Commanders to develop "campaign plans as appropriate to address their regional or functional responsibilities."[15] The campaign plan "integrates security cooperation, Phase 0, and other steady-state activities, with operations and contingency plans to attain immediate objectives that contribute to the broad, strategic end states established in the GEF."[16] The JSCP and GEF are complementary documents which must be reviewed together when conducting security cooperation planning. "The JSCP does not repeat the strategic end states or detailed security cooperation guidance found in the GEF."[17] The JSCP, however, does address "the combatant command's procedures for disclosing sensitive or classified U.S. military information to allied, coalition, or partner personnel" under general planning guidance for coalition operations.[18] Foreign disclosure is another significant issue that will be examined in the "Intelligence Sharing Challenges" section of this paper.

Finally, the QDR, National Strategy for Information Sharing, and Intelligence Community Information Sharing Strategy are indirectly related to the GCC's TSC planning and intelligence sharing activities. For example, the QDR discusses "increasing Maritime Domain Awareness through improved integration with interagency and international partners, and accelerated investment in multinational information sharing…."[19] The National Strategy for Information Sharing and the United States Intelligence Community Information Sharing Strategy are strategic level documents which are significantly changing the way U.S. government agencies and the U.S. Intelligence Community use and disseminate intelligence

and information. These policies are also easing restrictions on sharing intelligence and information on terrorism related issues with various foreign partners.[20]

VALUE OF SHARING INTELLIGENCE AND INFORMATION

Intelligence sharing is a critical component of TSC and multinational operations for several reasons. First, it enables GCCs to make better informed operational decisions. Second, it provides access to unique sources of information, capabilities, and Intelligence Surveillance and Reconnaissance (ISR) assets. Third, it is an effective tool in combating terrorism. Fourth, it promotes unity of effort. Finally, it supports greater security cooperation objectives.

Joint Publication 2-0 "*Joint Intelligence*" lists "Inform the Commander" as the primary purpose of joint intelligence. Intelligence reporting and analysis provided by foreign partners contribute to the collective knowledge and understanding of the threat.[21] With greater situational awareness and understanding of the threat, GCCs are able to make better informed operational decisions.

Intelligence sharing provides access to unique sources of information, especially HUMINT. While the U.S. has a superior ability to collect intelligence by technical means, HUMINT collection capabilities are limited due to "insufficient numbers of linguists, difficulty in accessing certain countries, and challenges infiltrating tribal organizations."[22] Many foreign partners do not have means for technical intelligence collection, but instead rely heavily on robust HUMINT collection networks. Partner HUMINT programs are able to more easily gain valuable intelligence because language, culture, ethnicity, and religion are usually not limiting factors. In addition, some partner countries may have access to unique capabilities or ISR assets which can contribute to the overall intelligence picture. Other

partners may be able to gain valuable intelligence due to their strategic location. For example, Singapore and Panama can provide unique intelligence which supports Maritime Domain Awareness due to their physical location along the Malacca Strait and Panama Canal respectively. GCCs can access these unique sources of intelligence only through intelligence sharing agreements with partner nations.

There are many uses for intelligence across the ROMO. Intelligence is particularly important, however, when conducting irregular warfare operations such as combating terrorism and counter-insurgency. The DoD Irregular Warfare Joint Operating Concept defines irregular warfare as "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations."[23] It further states that "irregular warfare is about people, not platforms. Irregular warfare depends not just on our military prowess, but also our understanding of such social dynamics as tribal politics, social networks, religious influences, and cultural mores."[24] Since insurgents and terrorists "hide among civilians and rely on them for support, persuading these non-combatants to provide government agencies with human intelligence on the identity, location, and activities of insurgents" is crucial in combating their activities.[25] "The war on terror requires high levels of intelligence to identify a threat relative to the amount of force required to neutralize it. This fact elevates intelligence in importance and places it on the frontline against terrorism."[26] Our partners can help us immensely in this area since they interact with the local population and are better positioned to collect HUMINT, which is essential in executing irregular warfare operations.

Intelligence sharing is a critical component of TSC and multinational operations because it promotes unity of effort. Joint Publication 3-16 "*Multinational Operations*" states that "a threat to one element of an alliance or coalition by the common adversary must be

considered a threat to all alliance or coalition elements."[27] Intelligence sharing promotes unity of effort among coalition partners by ensuring the leadership has a common understanding of the enemy threat which helps synchronize operational efforts and enhances force protection.

Finally, intelligence sharing enables GCCs to achieve other security cooperation objectives. U.S. intelligence is provided to a partner in exchange for intelligence collected and analyzed by the partner, but this is not the only way intelligence sharing provides GCCs value. U.S. intelligence may be shared for reasons other than simply receiving foreign intelligence reporting in return. For example, intelligence may be provided to a partner so that they can take some action beneficial to the U.S., such as capturing a terrorist operating in the partner's country. Alternatively, GCCs can use intelligence sharing as a bargaining chip when negotiating with partners for privileges such as basing rights and overflight of national airspace. Conversely, foreign partners may offer to share intelligence with the U.S. in certain situation when they cannot offer more tangible or public contributions to a coalition for either financial or political reasons.[28] The quid pro quo for intelligence sharing in each partnership is unique, but whether tangible or intangible, intelligence sharing provides GCCs value.

INTELLIGENCE SHARING CHALLENGES

There are several complex challenges associated with intelligence sharing. While not insurmountable, GCCs and J-2s must proactively address these issues in order to effectively leverage intelligence sharing programs. If the challenges are not adequately addressed, GCCs and J-2s risk alienating partners and damaging intelligence sharing efforts.

Intelligence sharing relationships must be built on mutual trust and take a significant amount of time to develop. In order to effectively build trust, GCCs, J-2s, and supporting

staffs must truly value the relationship and be willing to invest a significant amount of time and effort into developing it. They must foster strong personal relationships with their counterparts and gain a deep understanding of their partner's security concerns.[29] Continuous communications and interactions over an extended period of time are also essential.[30] GCCs, J-2s, and supporting staffs, however, have numerous day-to-day duties and responsibilities which compete for their time and often receive higher priority. In an environment with numerous competing requirements, it is easy to deemphasize security cooperation and intelligence sharing activities with partners. This is coupled with the fact that GCCs and J-2s engage numerous partner nations within their AOR. Furthermore, inadequate funding and lack of dedicated personnel for TSC activities give the perception that the relationship is not valued.[31] If intelligence sharing relationships are not continuously reaffirmed, trust will erode, and the quality and quantity of intelligence provided by the partner nation will diminish.

The issue of trust, or more appropriately mistrust, is compounded when intelligence sharing is elevated from a bilateral to a multilateral framework. In this case, it is not just a single relationship between GCCs or J-2s and their counterparts that must be developed. Instead, it involves multiple high-level relationships between counterparts of many nations. For example, Admiral Michael Mullen, as U.S. Chief of Naval Operations, promoted a "Thousand Ship Navy" concept in which partner navies would work together and share information about threats at sea.[32] While few argue that greater cooperation is beneficial, several foreign military services cited "mistrust among nations" as a specific problem of implementing the plan.[33] According to one former senior naval officer, "Everyone wants to see the common operating picture, but they aren't necessarily willing to contribute to it. The

guy next door might be watching, and we don't want him to see what we are doing. Those local issues of suspicion are probably going to translate into problems."[34] The theme of mistrust among nations was echoed in a May 2007 interview with the International Security Assistance Force (ISAF) Intelligence chief, Canadian Army Brigadier General Jim Ferron. According to General Ferron, there are still information sharing challenges among the 37 ISAF member nations. "Every nation has its own methods and procedures for gathering intelligence, something they are not keen to share.… But the biggest lesson is that this environment is providing the means to [change] that."[35] Mutual trust must be developed through continuous interaction over time in order for intelligence sharing relationships to be effective. In other words, "The level of trust… and diplomatic relations… determine the extent to which intelligence is shared."[36]

Cultural and language differences can cause misunderstandings and or miscommunications which have negative consequences in intelligence sharing relationships. "As Americans, we often get right down to business and bypass informality. This is not the case in many other cultures of the world.… We can easily be unaware of the unique cultures of our long-standing allies and not be as effective as possible in coordination."[37] In addition, miscommunication or incorrect translation of a partner's intelligence report may lead to misinformed operational decisions. J-2s and supporting staffs must have an appreciation for cultural differences when developing intelligence sharing relationships. Furthermore, J-2s must ensure U.S. personnel with appropriate language skills are available to facilitate the development of intelligence sharing relationships.

J-2s are challenged by complex foreign disclosure policies and processes that cause inefficiencies and limit intelligence dissemination. Joint Publication 2-0 states that the policy

and procedures for a particular operation must be based on the *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations* (NDP 1).[38] While NDP 1 serves the very important function of protecting intelligence as a U.S. national asset, it also establishes strict guidelines by which intelligence can be released to foreign nations. Joint Publication 2-0 states that it is incumbent upon J-2s to determine what intelligence may need to be shared early in the planning process.[39] Although, Joint Publication 2-0 also states that all necessary information should be shared, "information about intelligence sources and methods should not be shared with allies and coalition partners until approved by the appropriate national-level agency."[40] The guidelines set forth in NDP-1 and Joint Publication 2-0 require J-2s to perform numerous time-consuming administrative tasks before intelligence can be shared with partner nations. It is therefore critically important that J-2s have an appropriate number of qualified Foreign Disclosure Officers (FDOs) on the staff to work these high-visibility issues. Joint Publication 2-0 emphasizes this point by stating that "special attention should be paid to the intelligence classification level of access of multinational personnel. To this end, J-2s should consider adding extra [FDO] billets to facilitate information sharing."[41] Lack of qualified FDO support slows the intelligence sharing process and negatively affects intelligence sharing relationships with foreign partners.

An additional intelligence sharing challenge is that secure and interoperable information systems are not always available to foreign partners. Joint Publication 2-0 states that "the success of joint and multinational operations and interagency coordination hinges upon timely and accurate information and intelligence sharing."[42] It further states that "[combatant commanders] are responsible for the intelligence sharing architecture for their

commands."[43] Finally, Joint Publication 2-0 recognizes the Combined Enterprise Regional Information Exchange System (CENTRIX) as the current DoD multinational information sharing network.[44] However, there is little information available on how foreign partners acquire CENTRIX, who updates the classified cryptography, or provides maintenance and technical support once the system is installed at a foreign partner location. J-2s must work with the Director for Systems (J-6) to coordinate the overall employment of CENTRIX and specifically address the details of who handles the cryptography, who provides technical support, and who performs system maintenance and upgrades. Failure to ensure partners have a functional secure information system limits the ability to share intelligence, gives the impression that the relationship is not valued, and erodes trust.

The fact that many foreign partner militaries are not organized like the U.S. and do not operate jointly presents another intelligence sharing challenge. While many partners have some form of a joint headquarters, others are more service centric. GCCs and J-2s may not have a direct counterpart or may engage with national level military leaders. In some countries, intelligence is tightly controlled by the service who acquires the information. Therefore, it is important for the service component Directors for Intelligence (N-2, S-2, A-2, etc.) to develop service–to–service intelligence sharing agreements and personal relationships with their respective counterparts. Intelligence acquired through these agreements should ultimately be provided to the J-2.

Finally, the fact that some foreign partners lack training on U.S. security procedures or simply do not fully understand the importance of protecting classified intelligence, presents a significant challenge. Despite being releasable to foreign partners, classified intelligence and sensitive operational information must still be protected. Intelligence

sharing agreements must clearly state what level of protection a foreign partner is expected to provide the information shared. J-2s should reiterate security concerns and, if necessary, provide OPSEC and classified intelligence security training.

THE CASE AGAINST SHARING INTELLIGENCE

While there is general agreement that intelligence sharing provides significant benefit to GCCs, there are inherent risks that must be considered. Specifically, counterintelligence threats and espionage are a fact of life in the intelligence business that cannot be overlooked. While intelligence sharing with foreign partners is important in combating terrorism and in other mission areas across the ROMO, it is important to remember that foreign partners will always act in their own national interests. Not all partners are equally friendly toward the U.S., and a partner in today's conflict may have different national interests in a future conflict. While the NDP-1 creates an administrative burden for GCCs and J-2s by requiring justification for the need to share intelligence, it serves the critical purpose of protecting intelligence as a national asset. GCCs and J-2s should carefully consider the reasons for sharing intelligence and provide strong justification.

Intelligence sources and analytical methods must always be protected because the compromise of sources and methods can lead improved enemy deception and denial efforts.[45] An example of this problem is covered in the book "*Combating Proliferation.*" The authors examine a case in which the U.S. government shared intelligence with the Russian government regarding Russian firms transferring nuclear and missile technology to Iran during the 1990's. The authors concluded that "as Russian officials learned of specific Israeli and U.S. intelligence capabilities, they evidently began to take steps to counter these intelligence sources."[46] While this example highlights an intelligence sharing issue at the

national level, the lesson of compromised sources and methods apply equally to all levels of intelligence sharing. Therefore, it is important that GCCs and J-2s do not enter an intelligence sharing relationship without thinking through potential pitfalls and coordinating with higher authorities in the U.S. Intelligence Community.

Finally, GCCs and J-2s must be on guard against false or politically motivated intelligence provided by partners.[47] For example, a partner nation facing an insurgency may provide inaccurate intelligence reporting which overestimates insurgent capacity to fight and underestimate its own military capabilities in order to justify requests for financial support or military assistance.[48] Again, foreign partners will always act in their own national interests and may falsify intelligence to achieve their national objectives.

In summary, a case can be made against establishing robust intelligence sharing relationships with foreign partners. Counterintelligence threats, inadvertent disclosure of U.S. sources and methods, and the potential for deception are inherent risks in an intelligence sharing relationship. But these risks can be mitigated through careful TSC planning, vigilance, and adherence to established security procedures. GCCs and J-2s need to weigh the benefits of an intelligence sharing relationship against the potential risks. By closely examining the dynamics of each relationship and setting specific intelligence sharing parameters, GCCs and J-2s can minimize risk while ensuring the intelligence necessary to achieve common objectives is appropriately shared.

CONCLUSIONS

In today's complex security environment, there are many threats that the U.S. military cannot tackle alone. Intelligence sharing with allies and foreign partners is a critical component of TSC that must be given greater focus by GCCs and J-2s. Intelligence sharing

must be made a priority in the overall security cooperation planning process and exercised at every opportunity.

Intelligence sharing agreements are valuable because they give GCCs the opportunity to leverage foreign partner intelligence assets, capabilities, and analysis in support of multinational operations. Intelligence sharing agreements also provide access to unique sources of information, specifically HUMINT, which help inform decisions.

Intelligence sharing relationships with partner nations must be built upon mutual trust and take a significant amount of time to develop. In order to effectively build trust, GCCs and J-2s must develop a strong personal relationship with their counterparts. Personal relationships significantly influence the quality and quantity of intelligence exchanged. GCCs and J-2s must also appreciate cultural differences, understand partner security concerns, and be willing to invest time, effort, and resources.

Intelligence sharing with foreign partners is a challenging task. In order for it to be successful, GCCs and J-2s must address issues such as complex foreign disclosure policies, organizational differences, and limited availability of secure information systems to foreign partners. In addition, GCCs and J-2s must seriously consider the counterintelligence threat posed by sharing intelligence and ensure U.S. intelligence sources and methods remain protected.

RECOMMENDATIONS

Build Mutual Trust. The importance of building mutual trust cannot be overstated. Mutual trust can only be built if both partners are seriously committed to a strong intelligence sharing relationship. The strength of an intelligence sharing relationship is a direct function

of the amount of time and effort put into the relationship. Therefore, GCCs and J-2s must invest personal time and effort, as well as dedicate personnel and resources toward addressing the numerous intelligence sharing challenges.

Exercise Intelligence Sharing. Many challenges addressed in this paper could be mitigated if intelligence sharing processes and procedures were established and practiced during peacetime exercises. Specifically, information system shortcomings as well as foreign disclosure process chokepoints could be identified early and improved prior to conflict. J-2s should coordinate with J-5s to ensure intelligence sharing is practiced during combined exercises at the operational and tactical level. While the degree of intelligence play will vary by partner, it should be exercised at every opportunity. Integrating intelligence sharing into multinational exercises also allows J-2s to gain a better appreciation of partner intelligence strengths and weaknesses. Once known, J-2 staffs can work to provide the partner with training and assistance as needed to improve their collection capacity and their analytical capabilities. J-2s may also coordinate with the service components and other DoD organizations to secure funding for training and equipment. Finally, exercises yield valuable lessons learned which drive improvements in the intelligence sharing processes.

Develop and Exchange Priority Intelligence Requirements. Joint Publication 2-0 defines Priority Intelligence Requirements (PIRs) as "an intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment."[49] J-2s should develop and formally exchange a list of PIRs that represent the GCC's interests. The PIRs will help guide what intelligence reporting is provided by the partners. Partners should also be encouraged to develop their own PIRs and provide them to the J-2.

Address Foreign Disclosure Issues. Foreign disclosure policies must be clearly written and understood in order to ensure maximum exchange of intelligence while simultaneously preventing security violations. Policies that unnecessarily delay or prevent dissemination of intelligence reporting should be rewritten. Foreign disclosure processes should also be reviewed to ensure maximum efficiency. J-2s must ensure that all intelligence necessary to accomplish mission objectives is shared while information on sources and methods is protected. To accomplish this task, a sufficient number of qualified FDOs must be assigned to the J-2 staff.

U.S. Defense Attaché Coordination. GCCs and J-2s should closely coordinate intelligence sharing activities with the U.S. Defense Attaché (DATT). The DATT is "intimately familiar with the Ambassador or Chief of Mission's Mission Performance Plan (MPP), and can help the [GCC] direct his TSC plan toward projects and programs that will complement the MPP." [50] While primarily employed by the Defense Intelligence Agency, the DATT also represents the GCC in country and is in the perfect position to facilitate intelligence sharing relationships and liaison between the J-2 and foreign counterparts.

Update the GEF. As previously mentioned, the SCG used the term "Information Sharing/Intelligence Cooperation" which it defined as "activities that increase partner nation intelligence capacity, information sharing and awareness."[51] This term implies cooperation in conducting intelligence analysis, not just sharing intelligence reporting, a distinction that the GEF fails to make. Since the GEF replaced the SCG, the GEF should be updated to include this terminology.

NOTES

1. The act or process of intelligence and information sharing will be hereafter referred to simply as "intelligence sharing" unless quoting directly from a source that explicitly separates the two terms. Joint Publication 2-0 explains the difference between intelligence and information. "Information on its own is a fact or a series of facts that may be of utility to the commander, but when related to other information already known about the operational environment and considered in the light of past experience regarding an adversary, it gives rise to a new set of facts, which may be termed "intelligence." See Chairman, U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication (JP) 2-0 (Washington, DC: CJCS, 22 June 2007), 1-1.

2. U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008). (Secret) Information extracted is unclassified; and Chairman, US Joint Chiefs of Staff, *Joint Strategic Capabilities Plan FY 2008* (U), CJCSI 3110.01G, (Washington, DC: CJCS, 1 March 2008). (Secret) Information extracted is unclassified.

3. The GEF superseded the SCG along with several other guidance documents in 2008. See U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008). (Secret) Information extracted is unclassified.

4. U.S. President, *The National Security Strategy of the United States of America*, (Washington, DC: White House, 16 March 2006), 1.

5. Ibid., 37.

6. U.S. Department of Defense, *National Defense Strategy 2008*, (Washington, DC: Pentagon, June 2008), 15.

7. Chairman, US Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, (Washington, DC: CJCS, 2004), 17.

8. U.S. President, *Unified Command Plan* (U), (Washington, DC: White House, 17 December 2008), 6,8,10,13,17,19. (For Official Use Only) Information extracted is unclassified.

9. U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008), 5. (Secret) Information extracted is unclassified.

10. Ibid., 46. (Secret) Information extracted is unclassified.

11. Ibid., 79. [weapons of mass destruction] added. (Secret) Information extracted is unclassified.

12. Ibid., 111. (Secret) Information extracted is unclassified.

13. U.S. Department of Defense, *Security Cooperation Guidance* (U), (Washington, DC: Pentagon, July 2007), 28. (Secret) Information extracted is unclassified.

14. Ibid., 31. (Secret) Information extracted is unclassified.

15. Chairman, U.S. Joint Chiefs of Staff, *Joint Strategic Capabilities Plan FY 2008* (U), CJCSI 3110.01G, (Washington, DC: CJCS, 1 March 2008), E-2. (Secret) Information extracted is unclassified.

16. Ibid., E-1. (Secret) Information extracted is unclassified.

17. Ibid., G-1. (Secret) Information extracted is unclassified.

18. Ibid., F-4, F-5. (Secret) Information extracted is unclassified.

19. U.S. Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: Pentagon, 6 February 2006), 58.

20. U.S. President, *The National Strategy for Information Sharing*, (Washington, DC: White House, October 2007), 25; and U.S. Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*, (Washington, DC: ODNI 22 February 2008), 3.

21. Chairman, U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication (JP) 2-0 (Washington, DC: CJCS, 22 June 2007), 1-3.

22. Derek S. Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," Orbis 50, no. 3 (Summer 2006): 454.

23. U.S. Department of Defense, *Irregular Warfare, Joint Operating Concept*, (Washington DC: Pentagon, September 2007), 1.

24. Ibid.

25. James Igoe Walsh, "Intelligence Sharing for Counter-Insurgency," *Defense & Security Analysis* 24, no. 3 (September 2008): 282. http://www.ebsco.com/ (accessed 9 April 2009).

26. Reveron, "Old Allies, New Friends," 455.

27. Chairman, U.S. Joint Chiefs of Staff, *Multinational Operations*, Joint Publication (JP) 3-16, (Washington, DC: CJCS, 07 March 2007), 3-13.

28. Reveron, "Old Allies, New Friends," 456.

29. Bart Howard, "Preparing Leaders for Multinational Operations," Army, March 2008, 23.

30. Chairman, U.S. JCS, *Joint Intelligence*, 5-5.

31. Gregory L. Hager, "Supporting and Integrating Theater Security Cooperation Plans" (Carlisle, PA: US Army War College, 3 May 2004), 8-9. http://www.dinfos.dma.mil/DinfosWeb/JSPAC/SupportingandIntegratingTheaterSecurityCooperationPlans.pdf. (accessed 25 February 2009); and Gregory J. Dyekman, *Security Cooperation: A Key to the Challenges of the 21st Century,* (Carlisle, PA: Strategic Studies Institute, US Army War College, November 2007), 6. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub820.pdf. (accessed 25 February 2009).

32. Christopher P. Cavis, "SPANNING THE GLOBE; US Floats Fleet Cooperation Concept to Allies," *Defense News,* 08 January 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

33. Ibid.

34. Ibid.

35. David Pugliese, "ISAF Forces Broaden Intelligence-Sharing," *Defense News,* 21 May 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

36. Reveron, "Old Allies, New Friends," 457.

37. Howard, "Preparing Leaders," 23.

38. Chairman, U.S. JCS, *Joint Intelligence*, 5-2.

39. Ibid., 5-3.

40. Ibid., 5-3. The "appropriate" national-level agency which has the authority to release information on sources and methods depends on the type information, but is usually the agency which collected the information or authored the intelligence report.

41. Ibid., 5-13.

42. Ibid., 5-1.

43. Ibid.

44. Ibid., 5-13.

45. John D. Ellis and Geoffrey D. Kiefer, *Combating Proliferation: Strategic Intelligence and Security Policy* (Baltimore, MD: John Hopkins University Press, 2004), 124; and Reveron, "Old Allies, New Friends,"458.

46. Ellis and Kiefer, *Combating Proliferation*, 122.

47. Reveron "Old Allies, New Friends," 458.

48. Walsh, "Intelligence Sharing for Counter-Insurgency," 284.

49. Chairman, U.S. JCS, *Joint Intelligence*, GL-15.

50. Paul Sigler, "Defense Attachés and Theater Security Cooperation: Bringing Military Diplomacy into the 21st Century" (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007), 3.

51. U.S. Department of Defense, *Security Cooperation Guidance* (U), (Washington, DC: Pentagon, July 2007), 31. (Secret) Information extracted is unclassified.

BIBLIOGRAPHY

Cavis, Christopher P. "SPANNING THE GLOBE; US Floats Fleet Cooperation Concept to Allies." *Defense News,* 08 January 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

Dyekman, Gregory J. *Security Cooperation: A Key to the Challenges of the 21st Century*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, November 2007. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub820.pdf. (accessed 25 February 2009).

Ellis, John D., and Geoffrey D. Kiefer. *Combating Proliferation: Strategic Intelligence and Security Policy.* Baltimore, MD: John Hopkins University Press, 2004.

Hager, Gregory L. "Supporting and Integrating Theater Security Cooperation Plans." Carlisle, PA: U.S. Army War College, 3 May 2004. http://www.dinfos.dma.mil/DinfosWeb/JSPAC/SupportingandIntegratingTheaterSecurityCooperationPlans.pdf. (accessed 25 February 2009)

Howard, Bart. "Preparing Leaders for Multinational Operations." Army, March 2008. 21-24.

Pugliese, David. "ISAF Forces Broaden Intelligence-Sharing." *Defense News,* 21 May 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

Reveron, Derek S. "Old Allies, New Friends: Intelligence Sharing in the War on Terror." Orbis 50, no. 3 (Summer 2006): 453-68.

Sigler, Paul. "Defense Attachés and Theater Security Cooperation: Bringing Military Diplomacy into the 21st Century." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007.

U.S. Department of Defense. Guidance *for Employment of the Force 2008-2010* (U). Washington, DC: Pentagon, May 2008. (Secret) Information extracted is unclassified.

_____. *Irregular Warfare, Joint Operating Concept*. Washington DC: Pentagon, September 2007.

_____. *National Defense Strategy 2008*. Washington, DC: Pentagon, June 2008.

_____. *Quadrennial Defense Review Report*. Washington, DC: Pentagon, 6 February 2006.

_____. *Security Cooperation Guidance* (U). Washington, DC: Pentagon, July 2007. (Secret) Information extracted is unclassified.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Intelligence*. Joint Publication (JP) 2-0. Washington, DC: CJCS, 22 June 2007.

_____. *Joint Operations.* Joint Publication (JP) 3-0. Washington, DC: CJCS, 13 February 2008 with change 1.

_____. Joint Operation Planning. Joint Publication (JP) 5-0. Washington, DC: CJCS, 26 December 2006.

_____. *Joint Strategic Capabilities Plan FY 2008* (U). CJCSI 3110.01G. Washington, DC: CJCS, 1 March 2008. (Secret) Information extracted is unclassified.

_____. *Multinational Operations.* Joint Publication (JP) 3-16. Washington, DC: CJCS, 07 March 2007.

_____. *The National Military Strategy of the United States of America*. Washington, DC: CJCS, 2004.

U.S. Office of the Director of National Intelligence. *United States Intelligence Community Information Sharing Strategy*. Washington, DC: ODNI 22 February 2008.

U.S. President. *Unified Command Plan* (U). Washington, DC: White House, 17 December 2008. (For Official Use Only) Information extracted is unclassified.

_____. *The National Security Strategy of the United States of America.* Washington, DC: White House, 16 March 2006.

_____. *The National Strategy for Information Sharing.* Washington, DC: White House, October 2007.

Walsh, James Igoe. "Intelligence Sharing for Counter-Insurgency," *Defense & Security Analysis* 24, no. 3 (September 2008): 281- 301. http://www.ebsco.com/ (accessed 9 April 2009).

[1] The act or process of intelligence and information sharing will be hereafter referred to simply as "intelligence sharing" unless quoting directly from a source that explicitly separates the two terms. Joint Pub 2-0 explains the difference between intelligence and information. "Information on its own is a fact or a series of facts that may be of utility to the commander, but when related to other information already known about the operational environment and considered in the light of past experience regarding an adversary, it gives rise to a new set of facts, which may be termed "**intelligence**." See Chairman, U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication (JP) 2-0 (Washington, DC: CJCS, 22 June 2007), 1-1.

[2] U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008). (Secret) Information extracted is unclassified; and Chairman, US Joint Chiefs of Staff, *Joint Strategic Capabilities Plan FY 2008* (U), CJCSI 3110.01G, (Washington, DC: CJCS, 1 March 2008). (Secret) Information extracted is unclassified.

[3] The GEF superseded the SCG along with several other guidance documents in 2008. See U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008). (Secret) Information extracted is unclassified.

[4] U.S. President, *The National Security Strategy of the United States of America*, (Washington, DC: White House, 16 March 2006), 1.

[5] Ibid., 37.

[6] U.S. Department of Defense, *National Defense Strategy 2008*, (Washington, DC: Pentagon, June 2008), 15.

[7] Chairman, US Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, (Washington, DC: CJCS, 2004), 17.

[8] U.S. President, *Unified Command Plan* (U), (Washington, DC: White House, 17 December 2008), 6,8,10,13,17,19. (For Official Use Only) Information extracted is unclassified.

[9] U.S. Department of Defense, *Guidance for Employment of the Force 2008-2010* (U), (Washington, DC: Pentagon, May 2008), 5. (Secret) Information extracted is unclassified.

[10] Ibid., 46. (Secret) Information extracted is unclassified.

[11] Ibid., 79. [weapons of mass destruction] added. (Secret) Information extracted is unclassified.

[12] Ibid., 111. (Secret) Information extracted is unclassified.

[13] U.S. Department of Defense, *Security Cooperation Guidance* (U), (Washington, DC: Pentagon, July 2007), 28. (Secret) Information extracted is unclassified.

[14] Ibid., 31. (Secret) Information extracted is unclassified.

[15] Chairman, U.S. Joint Chiefs of Staff, *Joint Strategic Capabilities Plan FY 2008* (U), CJCSI 3110.01G, (Washington, DC: CJCS, 1 March 2008), E-2. (Secret) Information extracted is unclassified.

[16] Ibid., E-1. (Secret) Information extracted is unclassified.

[17] Ibid., G-1. (Secret) Information extracted is unclassified.

[18] Ibid., F-4, F-5. (Secret) Information extracted is unclassified.

[19] U.S. Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: Pentagon, 6 February 2006), 58.

[20] U.S. President, *The National Strategy for Information Sharing*, (Washington, DC: White House, October 2007), 25; and U.S. Office of the Director of National Intelligence, *United States Intelligence Community Information Sharing Strategy*, (Washington, DC: ODNI 22 February 2008), 3.

[21] Chairman, U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication (JP) 2-0 (Washington, DC: CJCS, 22 June 2007), 1-3.

[22] Derek S. Reveron, "Old Allies, New Friends: Intelligence Sharing in the War on Terror," Orbis 50, no. 3 (Summer 2006): 454.

[23] U.S. Department of Defense, *Irregular Warfare, Joint Operating Concept*, (Washington DC: Pentagon, September 2007), 1.

[24] Ibid., 1.

[25] James Igoe Walsh, "Intelligence Sharing for Counter-Insurgency," *Defense & Security Analysis* 24, no. 3 (September 2008): 282. http://www.ebsco.com/ (accessed 9 April 2009).

[26] Reveron, "Old Allies, New Friends," 455.

[27] Chairman, U.S. Joint Chiefs of Staff, *Multinational Operations*, Joint Publication (JP) 3-16, (Washington, DC: CJCS, 07 March 2007), 3-13.

[28] Reveron, "Old Allies, New Friends," 456.

[29] Bart Howard, "Preparing Leaders for Multinational Operations," Army, March 2008, 23.

[30] Chairman, U.S. JCS, *Joint Intelligence*, 5-5.

[31] Gregory L. Hager, "Supporting and Integrating Theater Security Cooperation Plans" (Carlisle, PA: US Army War College, 3 May 2004), 8-9. http://www.dinfos.dma.mil/DinfosWeb/JSPAC/SupportingandIntegratingTheaterSecurityCooperationPlans.pdf. (accessed 25 February 2009); and Gregory J. Dyekman, *Security Cooperation: A Key to the Challenges of the 21st Century*, (Carlisle, PA: Strategic Studies Institute, US Army War College, November 2007), 6. http://www.strategicstudiesinstitute.army.mil/pdffiles/pub820.pdf. (accessed 25 February 2009).

[32] Christopher P. Cavis, "SPANNING THE GLOBE; US Floats Fleet Cooperation Concept to Allies," *Defense News*, 08 January 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

[33] Ibid.

[34] Ibid.

[35] David Pugliese, "ISAF Forces Broaden Intelligence-Sharing," *Defense News*, 21 May 2007. http://www.lexis-nexis.com/ (accessed 9 April 2009).

[36] Reveron, "Old Allies, New Friends," 457.

[37] Howard, "Preparing Leaders," 23.

[38] Chairman, U.S. JCS, *Joint Intelligence*, 5-2.

[39] Ibid., 5-3.

[40] Ibid., 5-3. The "appropriate" national-level agency which has the authority to release information on sources and methods depends on the type information, but is usually the agency which collected the information or authored the intelligence report.

[41] Ibid., 5-13.

[42] Ibid., 5-1.

[43] Ibid.

[44] Ibid., 5-13.

[45] John D. Ellis and Geoffrey D. Kiefer, *Combating Proliferation: Strategic Intelligence and Security Policy* (Baltimore, MD: John Hopkins University Press, 2004), 124; and Reveron, "Old Allies, New Friends,"458.

[46] Ellis and Kiefer, *Combating Proliferation*, 122.

[47] Reveron "Old Allies, New Friends," 458.

[48] Walsh, "Intelligence Sharing for Counter-Insurgency," 284.

[49] Chairman, U.S. JCS, *Joint Intelligence*, GL-15.

[50] Paul Sigler, "Defense Attachés and Theater Security Cooperation: Bringing Military Diplomacy into the 21st Century" (research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2007), 3.

[51] U.S. Department of Defense, *Security Cooperation Guidance* (U), (Washington, DC: Pentagon, July 2007), 31. (Secret) Information extracted is unclassified.